UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,662	03/31/2004	Naoki Naruse	9683/183	5965

757   7590   02/20/2008
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER
POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
02/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/814,662	NARUSE ET AL.
Office Action Summary	Examiner	Art Unit	
	PETER POLTORAK	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *04 December 2007*.

2a) ☒ This action is FINAL.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1 and 7-29* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1 and 7-29* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *12/04/07* is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All   b) ☐ Some * c) ☐ None of:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____.

        3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Applicant amendments and drawings received on 12/04/07 have been accepted.

Response to Arguments

2. In light of applicant's amendments and arguments the objections to drawings and
   Oath/Declaration as well as 35 USC § 101 and 112 rejections are withdrawn.

3. Applicant's arguments have been considered but are moot in view of the new
   ground(s) of rejection.

4. Claims 1-29 have been examined.

   The text of those sections of Title 35, U.S. Code not included in this action can be
   found in a prior Office action.

Objections

5. Claim 18 is objected to because "The first file" in claim 18 lacks antecedent basis
   (and consistency, see "<u>a</u> second file" and "<u>a</u> third file" following "<u>the</u> first file").
   Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. Claims 1, 7-11, 15, 17-23, 27, 29 are rejected under 35 U.S.C. 103(a) as obvious
   over Stallings (William Stallings, "Cryptography and network security", 2th edition,
   1998, ISBN: 0138690170) in view of Angelo (USPUB 2003/0061487).

Stallings discloses a first file (message M) and a third file (hash of the first file:

H(MIIS) that is put together in a second file, illustrated as a two color rectangle in

Fig. 8.5 (e), for example.

As per claims 1, 7, 11, 18-19, 23 the examiner interprets the first file to read on

application data, bits value in the second file to read on the application validity data

and bits value in the third file as a second file validity data.

As seen in Fig. 8.5 (e) a communication device (Destination) receives the first,

second and third values. At least a part of the second file (the first file: M of the first

file comprising M and H(MIIS)) is input at the Destination to the one-way function to

generate the second file calculated value (H). The examiner interprets the result of

the calculation as a second file calculated value. As clearly disclosed in Fig. 8.5 (e)

the second file calculated value is compared with the second file validity data in the

third file. Since a one-way function uniquely identifies data, the comparison

inherently enables determining whether the second file is valid based on the second

file calculated value with the second file validity data in the third file.

An ordinary artisan would readily recognize the application validity data (the second

file) inherently verifies whether the application data (M) in the second file is valid,

and, since hash (H) is derived from M a positive comparison ensure that the second

file is valid. (Putting in plain language if a hash appended to and derived from a

message equal to a copy of hash newly generated the message, the message and

the original hash are verified to be valid.)

In other way to look at it is to say that, if the second file (M and H(MIIS), that is both M and H are valid) it verifies that the application data in the first file (M) is valid and as it was established above, this validity would have to been established using the application validity data in the second file (H).

Stallings is silent in regard to executing the application data on the communication device if above discussed validities are established, or putting simply, when a message and the associated hash are valid.

Angelo (USPUB 2003/0061487) discloses executing application data (which is a program) when it is determine that a message and the associated hash are valid (Angelo, [22]).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to execute the application data if the message and the hash are valid. One of ordinary skill in the art would have been motivated to perform such a modification in order to increased system's security.

7. Claims 8-10, 15, 20-22 and 27 recite the same inherent features of the discussed above message authentication using a message hash, and as per claim 22, an ordinary artisan would readily recognize that in other to derive the same hash of the message the hash function must be the same (see text associate with Fig. 8.5 (e) on pg. 247.

8. As per the limitation of claims 17 and 29, the examiner points out that in the situations where a file comprises more than one file, additional data must be included in order to enable a proper interpretation of values, that is in order to

identify which values belong to which data, or in other words, how to read and

interpret the received data. This additional data identifies location of particular parts

of the data (note that the location can be identified either explicitly, the end of data or

the beginning of new data, or not explicitly, a type of protocol used which

distinguishes which anticipate a particular location for a particular data). The

examiner interprets this additional data to be a part of the second file.

9. Claims 1, 7-13, 15, 18-25 and 27 are rejected under 35 U.S.C. 103(a) as obvious

over Angelo (USPUB 2003/0061487) in view of Feghhi (Jalal Feghhi, Jalil Feghhi,

Peter Williams, "Digital Certificates Applied Internet Security, 1999, ISBN:

0201309807).

The examiner refers to one-way function as hash or hash function, which is

consistent with the practice in the art of computer security.

10. Angelo discloses executing application data (which is a program) when it is

determine that a message and the associated hash, or a digital signature (to be

more exact) are valid (Angelo, [22]).

In paragraphs 22-23 Angelo discloses as follows:

"In accordance with the preferred embodiment of the invention,

however, the operating system preferably performs the following security

feature, or otherwise causes the following security feature to be performed.

The workstation computer on which the application is to run preferably computes

a hash of the copy of the object code to be executed thereon. The hash

function used by the computer preferably is the same hash function that was

used to create hash H1 stored in the security database 110. The workstation

computer also retrieves the previously computed, signed hash H1 from the

security database corresponding to the program to be run. The computer

decrypts the signed hash using a public key that corresponds to the private key

used to encrypt the hash in the first place.

The computer then compares the two hashes—the newly computed hash of

the particular copy of the object code to be executed and the previously

computed hash of presumably the same object code. If the object code has been

modified in any way, the newly computed hash will differ from the previously

computed hash. Accordingly, the computer 104-108 attempts to authenticate its

copy of the object code to be executed by comparing the two hashes. <u>If they

match, then computer determines that the object code is authentic, and then

proceeds with running the software.</u> "

A file comprising the application disclosed by Angelo reads on a first file comprising

the application data. A file storing a digital signature (signed hash) with associated

public key (for checking the signature) reads on a second file comprising application

validity data and running the software if computed signatures match as taught by

Angelo clearly shows that the application validity data is used to verify validity of the

application data in the first file and that the application data on the communication

device is executed if the application data is verified.

Angelo does not disclose a third file comprising second file validity data calculated

with a one-way function and used to verify the second file.

However, an ordinary artisan would readily recognize a security weakness of Angelo

invention. Specifically, even though the process disclosed by Angelo verifies data

application data authenticity it does not verify the source of the authentic data. The

reason would have been clear to an ordinary artisan: verification of the application

data in the first file depends on security of a public key that corresponds to a private key used in creating at the second file (the key signing the hash). A potential attacker could replace a legitimate file signing with its own private key and supplying the corresponding public key, and the verification process would also prove that the data (first file) is authentic. Of course, in this case the authentic data would be the data supplied by the attacker.

Feghhi discloses remedy to this potential security threat. Feghhi discloses a third file (a certificate, Fegghi, e.g. Fig. 3-2) that includes application validity data (Certification Authority's Digital Signature). As disclosed in Chapter 3 (pg. 61-89) Fegghi discloses that digital certificate authenticates subjects by binding the subject's public key to its identity (Fegghi, e.g. "X.509 Digital Certificates", pg. 65, "Subject Authentication", pg. 81, etc.). Since the certificate disclosed by Fegghi uses a public key to generate signature and signature is generated using hash of the data (that as seen in Fig. 3-2, includes the public key), the process of verifying the signature, that inherently includes comparing the original value (the second file validity data in the third file) with the second file calculated value (that is a value derived by hashing (inputting to one-way function) at least a part of the second file (the public key)).

Note that digital certificates are issued by Certification Authorities which are trusted organization (e.g. Fegghi, pg. 79-80). Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to provide a third file comprising application validity data given the benefit of increased security.

Verifying the second file based on comparing the second file calculated value with the second file validity data in the third file before executing the application data would have being implicit. As discussed before, verifying the second file based on comparing the second file calculated value ensures that the authentic data is generated by a certified subject/entity.

11. Claims 14, 16, 26 and 28 are rejected under 35 U.S.C. 103(a) as obvious over Angelo (USPUB 2003/0061487) in view of Feghhi (Jalal Feghhi, Jalil Feghhi, Peter Williams, "Digital Certificates Applied Internet Security, 1999, ISBN: 0201309807) in view of Fukumoto(USPUB 2002/0073072).

As discussed above, operations on the received second and third files determines validity of the second file, the third file (digital certificate) disclosed by Fegghi is provided by Certificate Authorities.

12. Angelo in view of Fegghi does not disclose that the second file is received from a content provider server and does not disclose that the receiver receives the first file only after determining validity of the second file.

In analogues art, Fukumoto discloses a receiver (terminal 10) using a certificate to receive application data (program P) from a content provider server (server 30). Fukumoto discloses that a first file is received after determining validity of a second file (Fukumoto, [58]). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure Angelo in view of Fegghi's system to receive the first file only after determining validity of the second file. One of ordinary skill in the art would have been motivated to perform such a modification given the

benefit of improved security. Note that determining validity of the second file in

addition to operating on the second file included operating on the third file.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Peter Poltorak whose telephone number is (571) 272-

3840. The examiner can normally be reached Monday through Thursday from 9:00

a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Peter Poltorak/

Examiner, Art Unit 2134

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134